

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DISTRICT

UNITED STATES OF AMERICA,)
)
 Plaintiff,)
)
 v.) No. 4:16-CR-258 CEJ (NAB)
)
 ALDEN DICKERMAN,)
)
 Defendant.)

GOVERNMENT'S RESPONSE TO DEFENDANT'S MOTION FOR FRANKS HEARING

Comes now the United States of America, by and through its attorneys, Richard G. Callahan, United States Attorney for the Eastern District of Missouri, and Colleen Lang, Assistant United States Attorney for said district, and files its Response to Defendant's Motion for a *Franks* hearing.

Defendant filed a motion and memorandum requesting a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978). In support of his motion, defendant alleges that the affiant's affidavit was inherently misleading and contained false statements and relevant omissions. As subsequently discussed in detail, these allegations are misplaced. Defendant fails to identify that any statements contained in the affidavits were deliberately or recklessly false. Nor does defendant show that omitted truthful statements, if supplemented in the affidavit, would have affected the probable cause determination. Accordingly, a showing has not been made to support a *Franks* hearing in this case.

I. FACTUAL BACKGROUND¹

A. Background on Freenet and Law Enforcement Investigations on Freenet

In September of 2011, Special Investigator (“S.I.”) Wayne Becker of the Dent County Sheriff’s Department began to collect “keys” and files of child pornography located and being shared on “Freenet.” In April of 2012, Special Investigator (“S.I.”) Wayne Becker of the Dent County Sheriff’s Department began to review logs for requests of files containing child pornography on Freenet in order to find individuals who were looking for and sharing child pornography on Freenet. Freenet is a type of peer-to-peer network software that allows users to share files over the Internet. It uses a decentralized, distributed data store to keep and deliver information. It is free and publicly available software for publishing and communicating on the Internet. Freenet’s focus is to provide a place on the Internet for free speech and anonymity. In Freenet, each file is made up of several blocks, or splits, that are stored independently of each other. To view a file, you must request all the blocks that are necessary to reconstruct it. The keys used to identify a block to retrieve are the hash values of the blocks. Users contribute to the network by giving bandwidth and a portion of their hard drive for storing files. Freenet transmits data between nodes, also known as peers. Freenet also stores data on the nodes. The process of finding a piece of data, or a place to store data, is called routing. Nodes are the computers running Freenet. A node in Freenet interacts directly with its directly connected peers. Each peer’s IP address is visible to a node, but a node does not learn the IP addresses of its peers’ peers. On the current version of Freenet, a node may have up to 142 peers. (See Exhibit 1, “Statistical Detection of Downloaders of Child Exploitation Materials in Freenet” for more detail

¹ This factual background is identical to the factual background laid out in the Government’s Response to Defendant’s Motion to Suppress Evidence. The factual summary provided is intended as a general guide and is not intended as a comprehensive statement of the government’s case.

on Freenet).

Researchers and law enforcement studied the Freenet open source code and analyzed activity on Freenet. Through their study they were able to create a statistical algorithm to determine the likelihood that a peer is the requestor of child pornography files, versus being a peer that only relayed the request. The timeline for these activities are as follows. Beginning in 2012, S.I. Becker collected keys in order to build database of files on Freenet that are associated with known or suspected child pornography images and videos. Researchers at the University of Massachusetts Amherst helped modify the Freenet program for law enforcement use. The modification logs the IP address, the content hash key values, the hops-to-live (“HTL”), types of requests, and the date/time of the requests as it passes through the node. Back in 2012 and 2013, this information was then collected by SI Becker’s ICAC lab in Salem, Missouri. SI Becker analyzed that information to determine if the IP address appeared to be the likely requester of known child pornography files on Freenet.

SI Becker began investigating child pornography offenders on Freenet in 2012 and 2013. In 2014, the research staff at University of Massachusetts Amherst worked with SI Becker to develop a new method to determine if an IP address appeared to be requesting known child pornography files on Freenet.

In 2015, these researchers developed a statistical algorithm for determining whether a peer is more likely to be requesting child pornographic material on Freenet or relaying such a request. This algorithm was still being refined at the time of SI Becker’s investigation into the defendant’s requests for child pornography on Freenet. At the time of investigation into the defendant, SI Becker was using a method that is fundamentally similar to what the algorithm does now because both methods count requests for blocks that make up a file of known child

pornography. A count of requests distinguishes the requesters from relayers.

While Freenet tries to be a harbor for anonymity, the website warns about the possibility that an IP address could be recognized. The website states, “If you are connected to a node, and can recognise the keys being requested (probably because it was posted publicly), you can show statistically that the node in question probably requested it, based on the proportion of the keys requested from that node, the locations of nearby nodes, the HTL on the requests and so on.”² The warning is basically what law enforcement is doing – recognizing known keys and determining whom is a requestor versus a relayer by the number of blocks being requested.

The mathematical algorithm that is currently in use for the law enforcement version of Freenet is laid out in further detail in the article, “Statistical Detection of Downloaders of Child Exploitation Materials in Freenet,” and was written in July of 2016. Exhibit 1. The method the algorithm uses is very similar to the method that SI Becker used in 2015. The article sums up the algorithm as follows, “[b]riefly, the algorithm works by looking at the cumulative number of requests for blocks corresponding to a distinct file of interest made by any single node. It then calculates whether the number of requests observed is most likely what we would expect to observe if the peer were the originator of the request or just replaying request on behalf of other nodes.” Ex. 1, page 4, section 4.

B. Instant Offense

While investigating Freenet requests on April 2, 2015, S.I. Becker came across a computer with an IP address in the state of Missouri that requested a file of known child

² Warning from the Freenet Project webpage (<https://wiki.freenetproject.org/FAQ>).

pornography. SI Becker documented the data related to that IP address' request for the file of child pornography on Freenet. Exhibit 2, SI Becker's Excel Spreadsheet. S.I. Becker collected the file and IP address information and sent it to Det. Michael Slaughter of the St. Louis County Police Department who sent a subpoena to AT&T Internet services to determine the subscriber information for that IP address. AT&T responded that the name and address of the subscriber was Janis Dickerman at 9524 Corregidor Drive, St. Louis, Missouri, 63134.

A computer search of the address revealed that Janis Dickerman had Ameren UE utilities in her name at that residence since 1959. A search warrant was prepared by Det. Slaughter and signed by St. Louis County Judge Borbonus on August 18, 2015. The search warrant stated "While reviewing requests received by undercover Freenet nodes, located in Missouri, SI Becker observed IP address 172.12.235.62 routing/or requesting suspected child pornography blocks. The number and timing of the requests was significant enough to indicate that the IP address was the apparent original requestor of the file." Exhibit 3, Search Warrant Affidavit, ¶ 6. "SI Becker observed that on April 2, 2015, between 11:08 p.m. UTC and 11:10 p.m. UTC a computer running Freenet software, at IP address 172.12.235.62, requested from Freenet law enforcement nodes 69 parts, or blocks, of the following file." Ex. 3, ¶ 7. The affiant then identified that file with its' name and unique SHA1 hash value. The file was then described as a folder containing seventeen (17) images of a young prepubescent child in a lascivious display of her genitals and being anally penetrated. In paragraphs twelve (12) through twenty-two (22) of the search warrant affidavit, Freenet was described and explained at length. Ex. 3.

The search warrant was executed by St. Louis County Police on August 18, 2015, at 9524 Corregidor Drive, St. Louis, Missouri. The defendant, Alden Dickerman, was the only person home during the execution of the warrant. After being read his *Miranda* warnings, the defendant

told police that he lived in the home with his mother (Janis Dickerman) and his sister. The defendant stated that he owned three computers including a laptop. He stated that he was only user of his laptop, which was password protected. Further, the defendant told Det. Slaughter that he had used Freenet software. When asked about downloading pornography from Freenet, the defendant asked for an attorney and questioning about the case ceased.

Meanwhile Det. Partney and S.I. Becker searched the home for computers and computer-related devices. They previewed the defendant's computers at the residence to see if they contained child pornography. These computers were located in the defendant's bedroom. Two of the defendant's computers did not contain child pornography. A third computer belonging to the defendant was an Asus laptop computer that was password protected. Detectives located a typed list of passwords in the defendant's bedroom and were able to use one of the passwords to access the Asus laptop. S.I. Becker determined the Asus laptop contained Freenet software and files of child pornography.

On August 21, 2015, S.I. Becker began a forensic review of the Asus laptop. S.I. Becker is a qualified forensic examiner. S.I. Becker located 597 images of child pornography and 43 videos of child pornography on the defendant's laptop computer's Hitachi hard drive. Freenet and the related Frost software were also located on the laptop. Frost is a group message board that relies on the Freenet peer-to-peer network. S.I. Becker also found that the defendant was subscribed to three boards on Frost, "pthc," "lolicam," and "hurtcore." The titles of the boards are indicative of child pornography. Many of the images and videos found on the laptop depicted prepubescent minor children, under the age of twelve, engaging in sexually explicit conduct. S.I. Becker noted that about thirty-two (32) of the images and nine (9) of the videos depicted the sex abuse of children as young as toddlers or infants. Many of the images and

videos also portrayed sadistic or masochistic conduct.

On June 22, 2016, a federal grand jury indicted the defendant on one count of Possession of Child Pornography in violation of Title 18 U.S.C. Section 2252(a)(5)(B).

II. LEGAL ANALYSIS

A *Franks* hearing should not be granted unless there is actual evidence that the search warrant was invalid.

“There is, of course, a presumption of validity with respect to the affidavit supporting the search warrant. To mandate an evidentiary hearing, the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine. There must be allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by an offer of proof.” *Franks v. Delaware*, 438 U.S. 154, 171 (1978).

The defendant has raised mere allegations in his motion that the affiant misrepresented the accuracy of his findings in the search warrant. The defendant has not provided factual evidence or data to back up these assertions. The defense has failed to meet its burden to prove that the presumed valid affidavit in support of the warrant was actually invalid.

It is well established that “to obtain relief under *Franks*, ‘a defendant must first demonstrate that the law enforcement official deliberately or recklessly included a false statement, or omitted a truthful statement from his warrant affidavit.’” *United States vs Mashek*, 606 F.3d 922, 928 (8th Cir.2010). see also *United States v. McIntyre*, 646 F.3d 1107, 1113-14 (8th Cir.2011)(quoting *Mashek*). Furthermore, before a defendant may receive such a hearing, the reviewing magistrate judge must determine that the allegedly false statement was necessary to the finding of probable cause. *Franks v. Delaware*, 438 U.S. 154 (1978); see also *United States v. Mashek*, 606 F.3d 922, 928 (8th Cir.2010)(citing *United States v. Reinholz*, 245 F.3d 765, 774 (8th Cir.2001); *United States v. Jansen*, 470F.3d 762, 765-66 (8th Cir. 2006); *United*

States vs. Sandoval-Rodriguez, 452 F.3d 984,988 (8th Cir. 2006).

“Allegations of negligence or innocent mistake will not suffice to demonstrate a recklessness or deliberate falsehood.” *Mashek*, 660 F.3d at 928 (citing *Franks*, 438 U.S. at 171). “In determining if ‘an affiant’s statements were made with a reckless disregard for the truth,’ the test is whether, after viewing all the evidence, that affiant must have entertained serious doubts as to the truth of his statement or had obvious reasons to doubt the accuracy of the information he reported.” *McIntyre*, 646 F.3d at 1114 (quoting *United States v. Butler*, 594 F.3d 955, 961 (8th Cir. 2010). “A showing of deliberate or reckless falsehood is not lightly met.” *Id.*

The defendant has not met his burden with regard to either prong of *Franks*. A *Franks* hearing should not be granted unless there is actual evidence that the search warrant was invalid. The search warrant is valid on its’ face. With respect to the allegation that Detective Slaughter’s affidavit was inherently misleading and contained false statements, defendant never proves how the statement is false. The defendant writes in their motion that the following statement from the search warrant affidavit was a false representation of the findings of SI Becker’s investigation, “[t]he number and timing of the requests was significant enough to indicate that the IP address was the apparent original requester of the file.” Defendant alleges that the significant number and timing of the requests could not have been apparent unless SI Becker independently verified the assumptions. SI Becker did verify the number and timing of the requests by tracking them in an Excel spreadsheet. Ex 2. This spreadsheet has been provided to the defendant along with two articles regarding how Freenet works. The number and timing of the requests was significant enough to determine the defendant was the requestor of the file. While using a law enforcement version of Freenet modified to passively log observations, SI Becker could observe the streams of data coming through Freenet from the defendant’s IP address. This significant data logged

included information such as the time and frequency of requests for certain files of interest from a node. Ex. 2. SI Becker then reviewed the significant data and calculate the percentage of even share. Ex. 2. The higher the percentage of even share and the more requests per second there are for a file of interest – the more likely the requests are coming from the requestor and not a forwarder. Ex. 1, Section 3 and Ex. 2. The defendant requested a file of interest titled, “April – Another Set 2 (set 2).zip,” on Freenet. Within 1 minute and 58 seconds the defendant requested the multiple blocks that together will make up the file. The law enforcement node, “LE #693,” received 69 requests for that file that when complete contains 783 data blocks. Thus, 8.81% of the minimum necessary requests went through the law enforcement node on Freenet from the defendant’s IP address. The defendant had an average of 56.9 peers during the period of investigation (which includes the law enforcement node). On average, each peer would expect to receive an even proportion (i.e. share) of requests. If the defendant had been a relay rather than a requestor, the law enforcement node would have received a much smaller percentage of the requests. The process was repeated three times for three separate files on three separate days. Ex. 2. SI Becker did verify the conclusion “that requests were significant enough,” and kept track of this verification in his notes. Therefore, the statement in the affidavit is not false, but true because it is the correct conclusion to be drawn from SI Becker’s investigation of the defendant on Freenet.

The defendant goes to assert that above quoted statement from the search warrant is a false representation because it *omits* that SI Becker independently verified his conclusions. SI Becker did verify the conclusion “that requests were significant enough” as detailed in the paragraph above. While this analysis performed by SI Becker was not in the search warrant, only the conclusion of it, that does not make the search warrant misleading. Not every detail of

an investigation needs to be contained in the search warrant. Omissions to the search warrant are different than misrepresentations and require a different two-step test. The defense “must prove first that facts were omitted with the intent to make, or in reckless disregard of whether they make, the affidavit misleading, and, second, that the affidavit, if supplemented by the omitted information, could not support a finding of probable cause.” *United States v. Allen*, 297 F.3d 790, 795 (8th Cir. 2002).

By supplementing the missing information into the search warrant, namely that SI Becker kept track of the probability of number and timings of the requests from defendant’s IP address on Freenet, it actually bolsters the probable cause for the search warrant, not decreases it. Further, the information is not misleading since it does not lead to a result other than the one described in the search warrant. The search warrant affidavit describes in paragraphs twelve (12) through twenty-two (22) how Freenet works. Ex. 3.

Defendant next argues that Detective Slaughter’s omission of the behavior of Freenet’s routing necessary to estimate the probability that the received requests originated from the peer they were received from (instead of forwarded from elsewhere) is based in part on how many requests are received. Defendant asserts that the routing behavior and how it was working on a particular day could affect the interpretation of the results. Defendant goes on to then allege that a potential for false positives was also omitted from the search warrant affidavit. In response, the routing was working correctly on April 2, 2015. SI Becker knows from his extensive experience on Freenet and how it works, that the routing and bandwidth had to have been working properly for several reasons. First, the defendant had an average of 59.6 peers on Freenet at the time of the request for the file titled, “April – Another Set 2 (set 2).zip.” The minimum number of peers on Freenet is ten peers. To have as many as 59.6 peers, as the defendant did, the routing and

bandwidth was working properly. Second, the timing of the blocks being received by the defendant after he requested them is significant. The requests for the blocks that make up the file were sent by the defendant were logged at being within one minute and fifty-eight seconds. Once the file is requested, Freenet locates blocks that make up the file on different nodes on Freenet. The blocks are then sent to the requestor and once the minimum number of blocks needed to create the file are received, then the file can then be downloaded by the requestor. Based on SI Becker's experience on Freenet, if the bandwidth was poor then the defendant would have had much less peers, closer to 10 or lower, and would not have requested the blocks of the file so quickly.

Third, the defendant alleges there is a potential for false positives that might have resulted and that should have been in the search warrant affidavit. In this case, false positives did not result. No false positive rate has been established for the exact method SI Becker was using in 2015, however, that method is very similar to the one documented in Ex. 1. In July of 2016, a false positive rate was estimated by the researchers from University of Massachusetts at Amherst for the method described in Exhibit 1. In a test sampling four months of data, they observed a false positive rate of 1.35%. Plus, in this case, both Freenet and child pornography files were located on the defendant's computer during the execution of the search warrant – confirming that the search warrant was not based on a false positive result. Further, SI Becker saw that the defendant's IP address requested and received child pornography files on Freenet on June 6, 2015, and June 13, 2015. Since defendant's IP address was seen downloading two more files of child pornography in June of 2015, the likelihood that the defendant's April 2, 2015 was a false positive or based on poor bandwidth is even more reduced. Ex. 2. The defendant makes a blanket statement not supported by any facts, that "false positives are likely to occur."

Steve Dougherty's affidavit is not sufficient to mandate an evidentiary hearing under *Franks*. The defense expert's affidavit never specifically points out that SI Becker's conclusions or analysis was incorrect. The defense expert, Steve Dougherty, states that the law enforcement modified version of Freenet "uses a large list of suspected illegal files and the behavior of Freenet's routing to estimate the probability that received requests originated from the peer they were received from instead of forwarded through the peer from a different one, based in part on how many requests are received from the peer relative to the file's total size." Defendant's Ex. B ¶ 11. "For the attack's estimation to be accurate, routing must be working well between the peers at that particular time." Defendant's Ex. B ¶ 12. Nowhere does Mr. Dougherty claim that the routings were not working effectively at that time of SI Becker's investigations. Further, as detailed above, SI Becker could tell from looking at the streams of data, the number of peers the defendant had, the frequency of the blocks being received, and the timing of file being received by the defendant, that the routing and bandwidth were working correctly.

There are no false statements in the search warrant affidavit. The omissions, which are basically the raw data backing up SI Becker's ultimate conclusions, only bolsters the probable cause when supplementing. Neither prong of the *Franks* test has been met and, therefore, the defendant is not entitled to a *Franks* hearing.

III. CONCLUSION

In conclusion, defendant fails to establish that any of the statements in the affidavit are deliberately false or made in reckless disregard for the truth. A *Franks* hearing should not be granted unless there is actual evidence that the search warrant was invalid. The search warrant is valid and there is no evidence otherwise. The omissions from the search warrant affiant would

not change the probable cause basis for the issuance of the search warrant once supplemented into the affidavit. The affidavit of Steve Dougherty submitted by the defendant also does not prove which statements in the affidavit are deliberately false or made with reckless disregard for the truth. The defendant has not met his burden of establishing the need for a *Franks* hearing. The defendant has not shown *any* falsehood nor any material or significant omission from the search warrant affidavit. Wherefore, the government respectfully requests this Court to overrule and deny defendant's motion for a *Franks* hearing.

Respectfully submitted,

RICHARD G. CALLAHAN
United States Attorney

s/ Colleen Lang
Colleen Lang, #56872MO
Assistant United States Attorney
111 South 10th Street, Room 20.333
St. Louis, MO 63102
(314) 539-2200

CERTIFICATE OF SERVICE

I hereby certify that on November 21, 2016, the foregoing was filed electronically with the Clerk of the Court. The foregoing was emailed to all counsel of record by the undersigned.

s/ Colleen Lang
Colleen Lang, #56872MO
Assistant United States Attorney

Freenet Target Files Summary

[Return to Detail Page](#)

IP Address:	172.12.235.62
Geo Location:	Saint Louis

File of Interest #1

File Name:	April - Anonther Set 2 (set 2).zip				
SHA1 Hash:	BODS262HHKS3VS4FLQSOAAVAWTOE5FAW				
Probable Manifest Key:					
Data Blocks	783				
	Overall Totals:	Filtered: 71 Rows	LE # 693		
First Block Observed:	2015/04/02 23:08:56	2015/04/02 23:08:56	2015/04/02 23:08:56		
Last Block Observed:	2015/04/02 23:10:54	2015/04/02 23:10:54	2015/04/02 23:09:45		
Overall Runtime:	0:01:58	0:01:58	0:00:49		
Average Peers	56.9	56.9	56.9		
Total Unique Requests Logged	69	69	69		
% of Total:	8.81%	8.81%	8.81%		
% of Even Share:	501%	501%	501%		
Frequency Group	2 Records per second:	10	10		
	3 Records per second:	2	2		
	4 Records per second:	1	1		
	5 Records per second:	1	1		
	6 or more records/sec:	4	4		

11/3/2016 14:25

Freenet Target Files Summary

[Return to Detail Page](#)

IP Address:	172.12.235.62
Geo Location:	Saint Louis

File of Interest #2

File Name:	melinda-fuck.avi
SHA1 Hash:	DP4CM2J7OXNWVZYPLGPAQCTVRMCAVGF7
Probable Manifest Key:	
Data Blocks	464



		Overall Totals:	Filtered: 68 Rows	LE # 14			
First Block Observed:		2015/06/04 04:45:36	2015/06/04 04:45:36	2015/06/04 04:45:36			
Last Block Observed:		2015/06/04 04:46:44	2015/06/04 04:46:44	2015/06/04 04:46:43			
Overall Runtime:		0:01:08	0:01:08	0:01:07			
Average Peers		51.1	51.1	51.1			
Total Unique Requests Logged		67	67	67			
% of Total:		14.44%	14.44%	14.44%			
% of Even Share:		738%	738%	738%			
Frequency Group	2 Records per second:	4	4	4			
	3 Records per second:	8	8	8			
	4 Records per second:	5	5	5			
	5 Records per second:	1	1	1			
	6 or more records/sec:						

11/3/2016 14:25

Freenet Target Files Summary

[Return to Detail Page](#)

IP Address:	172.12.235.62
Geo Location:	Saint Louis

File of Interest #3

File Name:	k@ty 2.mpg
SHA1 Hash:	5JJD6XOPC3W6VFPEOIAZ7W7TK4ILMR2Z
Probable Manifest Key:	
Data Blocks	623

		Overall Totals:	Filtered: 31 Rows	LE # 817			
First Block Observed:		2015/06/13 08:18:15	2015/06/13 08:18:15	2015/06/13 08:18:15			
Last Block Observed:		2015/06/13 08:19:09	2015/06/13 08:19:09	2015/06/13 08:19:09			
Overall Runtime:		0:00:54	0:00:54	0:00:54			
Average Peers		62.7	62.7	62.7			
Total Unique Requests Logged		31	31	31			
% of Total:		4.98%	4.98%	4.98%			
% of Even Share:		312%	312%	312%			
2 Records per second:		6	6	6			

Frequency Group	3 Records per second:	1	1	1	1	1	11/3/2016 14:25
	4 Records per second:	1	1	1	1	1	
	5 Records per second:						
	6 or more records/sec:						

Save FOI-1 Summary to PDF

Save FOI-2 Summary to PDF

Save FOI-3 Summary to PDF

30
6
3
3
12

12
24
15

30

183300

FILED

AUG 18 2015

STATE OF MISSOURI

COUNTY OF ST. LOUIS

}

} SS

}JOAN M. GILMER
CIRCUIT CLERK, ST. LOUIS COUNTYIn Division 35 Circuit Court of ST. LOUIS COUNTY**STATE OF MISSOURI**
SEARCH WARRANTTO ANY POLICE OFFICER OF ST. LOUIS COUNTY, STATE OF MISSOURI,
GREETINGS:

WHEREAS, Detective Michael Slaughter, DSN 3562, of the St. Louis County Police Department, on the 18 day of August, 2015 presented to Judge Bar Sm of Division 35 of the Circuit Court of the County of St. Louis, State of Missouri, his duly verified application and petition in writing as provided by law stating upon information and belief that certain items believed to be evidence of the commission of a crime and contraband consisting of child pornography, to wit:

Photographs, files and graphic images depicting sexual contact or a sexual performance including actual or simulated, normal or perverted acts of human masturbation, deviate sexual intercourse, sexual intercourse or physical contact with or touching of a person's clothed or unclothed genitals, pubic area, buttocks, anus, or the breast of a female in an act of apparent sexual stimulation or gratification and which has as one of its participants or portrays as an observer of such conduct, contact or performance, a child or minor under the age of 18, electronic data processing and storage devices, computers and computer systems including central processing units, internal peripheral storage devices such as fixed discs, external hard discs, floppy discs and diskettes, tape drives and tapes, optical storage device or other memory storage devices, peripheral input/output devices such as keyboards, printers, video display monitors, optical readers and related communication devices such as modems, routers and other wireless devices; any and all cameras and related equipment, video and audio recorders and all related recording equipment; any and all photographs, copies of photographs and any manufactured hard copy of images related to child pornography; any and all logs containing user names, passwords and documentation or other identifiers necessary to examine or operate items; together with system documentation, operating logs and handwritten notes related to user identifications, passwords and/or child pornography;

Are being kept and secreted in St. Louis County, Missouri upon the following premises:

9524 Corregidor Drive, St. Louis, Missouri, 63134 is a single family residence constructed of red brick, and a grey roof. The residence has a permanently affixed number 9524 mounted on a porch post in front of the residence. The front door is white in color.



In violation of the laws of the State of Missouri.

WHEREAS, from the facts set forth in said verified petition and attached affidavit, it is found by me that there is probable cause to believe that the laws of the State of Missouri are being violated at and in and upon the premises described above and that said items constitute evidence of the commission of a crime.

NOW, THEREFORE, these are to command you that you search the said premises above described within 10 days after the issuance of this warrant by day or night, and take with you, if need be, the power of your county, and, if said above described property of any part thereof be found on said premises by you, that you seize the same and take same into your possession, making a complete and accurate inventory of the property so taken by you in the presence of the person from whose possession the same is taken, if that be possible, and giving to such person a receipt for such property, together with a copy of this warrant, or, if no person be found in possession of said property, leaving said receipt and said copy upon the premises searched, and that you thereafter return the property so taken and seized by you, together with a duly verified copy of the inventory thereof and with your return to his warrant to this court to be herein dealt with in accordance with law. You are further commanded to search the computers, cameras, storage devices, and electronic devises seized by you, including any files that are password protected or encrypted, for evidence of ownership and usage, files and graphic images depicting child pornography depicting sexual contact or a sexual performance including actual or simulated, normal or perverted acts of human masturbation, deviate sexual intercourse, sexual intercourse or physical contact with or touching of a person's clothed or unclothed genitals, pubic area, buttocks, anus, or the breast of a female in an act of apparent sexual stimulation or gratification and which has as one of its participants or portrays as an observer of such conduct, contact or performance a child or minor, under the age of 18.

WITNESS my hand and seal of this court this 18 day of August, 2015 at 1405.



(Judge)

STATE OF MISSOURI }
 } SS
COUNTY OF ST. LOUIS }

In Division 35 Circuit Court of ST. LOUIS COUNTY

STATE OF MISSOURI
SEARCH WARRANT

TO ANY POLICE OFFICER OF ST. LOUIS COUNTY, STATE OF MISSOURI, GREETINGS:

In the matter of: **Search Warrant**

APPLICATION FOR SEARCH WARRANT

I, Detective Michael Slaughter, DSN 3562, of the St. Louis County Police Department, being duly sworn depose and state upon information and belief that the premises known, numbered and designated as:

9524 Corregidor Drive, St. Louis, Missouri, 63134 is a single family residence constructed of red brick, and a grey roof. The residence has a permanently affixed number 9524 mounted on a porch post in front of the residence. The front door is white in color.

is being used for the purpose of secreting:

evidence of the commission of a crime and contraband consisting of child pornography, to wit:

Photographs, files and graphic images depicting sexual contact or a sexual performance including actual or simulated, normal or perverted acts of human masturbation, deviate sexual intercourse, sexual intercourse or physical contact with or touching of a person's clothed or unclothed genitals, pubic area, buttocks, anus, or the breast of a female in an act of apparent sexual stimulation or gratification and which has as one of its participants or portrays as an observer of such conduct, contact or performance, a child or minor under the age of 18, electronic data processing and storage devices, computers and computer systems including central processing units, internal peripheral storage devices such as fixed discs, external hard discs, floppy discs and diskettes, tape drives and tapes, optical storage devise or other memory storage devices, peripheral input/output devices such as keyboards, printers, video display monitors, optical readers and related communication devices such as modems, routers and other wireless devices; any and all cameras and related equipment, video and audio recorders and all related recording equipment; any and all photographs, copies of photographs and any manufactured hard copy of images related to child pornography; any and all logs containing user names, passwords and documentation or other identifiers necessary to examine or operate items; together with system documentation, operating logs and handwritten notes related to user

identifications, passwords and/or child pornography;

That the basis of affiant's information and belief is contained in the attached affidavits of witnesses to facts concerning the said matter which affidavits are made a part hereof and are submitted herewith as a basis upon which this court may find the existence of probable cause for the issuance of said warrant.

WHEREFORE, your petitioner prays that a search warrant be issued as provided by law.


(Police Officer) 3847

Subscribed and sworn to before me this 18 day of August, 2015 at 1405.


(Prosecuting Attorney)


(Judge)

STATE OF MISSOURI }
 } SS
COUNTY OF ST. LOUIS }

AFFIDAVIT

This affiant, Detective Michael Slaughter, DSN 3562, of the St. Louis County Police Department of lawful age, being first duly sworn, deposes and says that he has reason to believe:

Photographs, files and graphic images depicting sexual contact or a sexual performance including actual or simulated, normal or perverted acts of human masturbation, deviate sexual intercourse, sexual intercourse or physical contact with or touching of a person's clothed or unclothed genitals, pubic area, buttocks, anus, or the breast of a female in an act of apparent sexual stimulation or gratification and which has as one of its participants or portrays as an observer of such conduct , contact or performance, a child or minor under the age of 18, electronic data processing and storage devices, computers and computer systems including central processing units, internal peripheral storage devices such as fixed discs, external hard discs, floppy discs and diskettes, tape drives and tapes, optical storage devise or other memory storage devices, peripheral input/output devices such as keyboards, printers, video display monitors, optical readers and related communication devices such as modems, routers and other wireless devices; any and all cameras and related equipment, video and audio recorders and all related recording equipment; any and all photographs, copies of photographs and any manufactured hard copy of images related to child pornography; any and all logs containing user names, passwords and documentation or other identifiers necessary to examine or operate items; together with system documentation, operating logs and handwritten notes related to user identifications, passwords and/or child pornography;

Are being kept and secreted in the place described as:

9524 Corregidor Drive, St. Louis, Missouri, 63134 is a single family residence constructed of red brick, and a grey roof. The residence has a permanently affixed number 9524 mounted on a porch post in front of the residence. The front door is white in color.

Affiant states that he has reason to believe such goods are being secreted therein because:

1. This Affiant, Detective Michael Slaughter, DSN 3562, has been employed as a Police Officer for approximately ten years, and is currently assigned as a Detective to the Division of Criminal Investigation, Special Investigations Unit with the St. Louis County Police Department. During the course of this time period, this affiant has had numerous contacts and dealings with informants, other police officers, subjects known to possess and sell obscene material, subjects known to possess, distribute and manufacture child pornographic images, adult subjects conducting sexually explicit electronic chat sessions with minors and visually exposing their genitals to the minor via web cam chats. This affiant has received specialized training in the area of computer-based investigations, including but not limited to the ICAC Investigative Techniques, ICAC Undercover Chat Techniques, ICAC Peer to Peer Investigations, TUX4n6 software, Forensic Scan, Cellebrite and OS Triage Forensic Tools. This affiant has assisted with investigations and search warrants relative to the crimes of manufacturing, possession, of electronic videos and images. This affiant is also familiar with investigating Cyber tip reports, conducting on-scene interviews and knock and talk techniques.

2. The statements in this affidavit are based in part on this affiant's personal knowledge or information provided by other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, your affiant has not included each and every fact concerning this investigation.

3. Special Investigator (SI) Wayne Becker is a certified Missouri Peace Officer employed as a sworn Deputy with Dent County Sheriff's Department since 2004. SI Wayne Becker has over 600 hours of training recognized and certified by the Missouri Peace Officers Standards and Training commission and has had over 450 additional hours of training, in the investigation of computer use in the exploitation of children, and in the methods of forensic analysis of computers used in criminal activity, including the use of peer-to-peer (P2P) and file sharing networks. SI Wayne Becker has an Associates of Science degree in Data Processing from St. Louis Community College, is a certified computer forensic examiner, has over 30 years of experience in the Information Technology industry, and is an instructor in Basic Electronic Evidence Recovery for the Missouri Internet Crimes Against Children (ICAC) Task Force. SI Wayne Becker is the Dent County Sheriff's Department's representative on the Missouri ICAC Task Force and coordinates the South Central Missouri Computer Crime Task Force.

4. This affiant received information from SI Wayne Becker, of the Dent County Sheriff's Department related to child pornography. SI Wayne Becker stated in September 2011, he began an undercover operation collecting keys and files being shared on a "*Freenet*", a publicly available peer to peer network, in order to build a data base of keys associated with known or suspected child pornography images and videos.

5. In April 2012, SI Wayne Becker began running copies of *Freenet* that had been modified for law enforcement to log the IP address, key, and date and time of requests that were sent to these law enforcement *Freenet* nodes. These keys are then compared to keys of known child pornography.

6. While reviewing requests received by undercover *Freenet* nodes, located in Missouri, SI Becker observed IP address 172.12.235.62 routing and/or requesting suspected child pornography file blocks. The number and timing of the requests was significant enough to indicate that the IP address was the apparent original requester of the file.

7. SI Becker observed that on April 2, 2015 between 11:08PM UTC and 11:10PM UTC a computer running *Freenet* software, at IP address 172.12.235.62, requested from Freenet law enforcement nodes 69 parts, or blocks, of the e following file:

SHA1: *BODS262HHKS3VS4FLQSOAAVAWTOE5FAW*

File Name: *Anonther Set 2 (set 2).zip*

SI Wayne Becker has downloaded this video file with the referenced SHA1 value from *Freenet* and it is described as follows:

Description: This folder contains 17 jpg images, all off a female child, 3-5 years of age. In all of the images she is wearing only a night shirt and it is pulled up. Her legs are spread displaying her genitals. An adult males hand can be seen spreading her buttocks for the camera in 2 of the images. In 4 of the images an unseen male's penis is penetrating the child anally.

8. On August 12, 2015 this affiant viewed the above listed files and observed that they contained the imagery described above that this affiant believes to be child pornography.

9. A subpoena was sent to AT&T Internet Services for user/subscriber information, to include method and type of payment for the IP address of 172.12.235.62 assigned on the above date and times. A response from AT&T Internet Services, advising that this was an AT&T U-Verse account and the IP address of 172.12.235.62 was assigned to Janis Dickerman as of September 24, 2014, giving a service and billing address of 9524 Corregidor Drive, Saint Louis, Missouri, 63134, with a telephone number of (314)651-9163.

10. An Ameren UE Utilities check revealed 9524 Corregidor Drive, St. Louis, Missouri, 63134, to be registered to Janis Dickerman, since 01/1959.

12. This affiant knows from training and experience that computer users can install publicly available software that accesses a network known as *Freenet*. *Freenet* is a distributed, Internet based, peer-to-peer network which lets a user anonymously share files and chat on forums. *Freenet* is free software and the source code is publicly available. Communications between computers running *Freenet*, or nodes, are encrypted and routed through other *Freenet* nodes making it difficult to determine who is requesting the information and what the content is of the information being requested. *Freenet* provides a platform for message forums and *Freesites*, websites only available through *Freenet*.

13. This affiant knows from training and experience that files, or parts of files, are stored in *Freenet* using a key created from a compressed digital representation method called Secure Hash Algorithm Version 256 or SHA256.

14. This affiant knows from training and experience that *Freenet* breaks a file into small pieces, or blocks, each with their own unique key based on this SHA256 value. These small blocks are then distributed across *Freenet* users, or nodes, and stored in disk space provided by each user to *Freenet*. No one user has the entire intact file. The keys to all of the parts of a file are found in a high level index block, or manifest.

15. This affiant knows from training and experience that Internet computers identify each other by an Internet Protocol or IP address. Your affiant knows that these IP addresses can assist law enforcement in finding the location of a particular computer on the Internet. These IP addresses lead the law enforcement officer to a particular Internet service provider or company (ISP). Given the date and time the IP address was used, an ISP can typically identify the account holder by name and physical address.

16. This affiant knows from training and experience that a computer running *Freenet* will receive requests from other computers running *Freenet* containing the key of a part of a file to retrieve from that node's data store, or to forward to another user that may have that part of the file.

17. This affiant knows from training and experience that *Freenet's* attempt to hide what a user is requesting from the network has attracted persons that wish to collect and/or share child pornography files. *Freenet* is not a significant source of music, adult pornography, theatrical movies or other copyright material.

18. This affiant knows from training and experience that *Freenet* users connect to other users, unknown to them, or peers. They then send requests to these peers for the blocks of files they are attempting to download.

19. This affiant knows from training and experience that the requests that a user of *Freenet* sends to a peer contain only the key for the block of data and not the encryption password to make the data readable. A user relies on the inability of a peer to decrypt a block of data or know what file contains this block to hide his use of the *Freenet* network to obtain child pornography files.

20. This affiant knows from training and experience that someone requesting blocks of a file has taken substantial steps to install *Freenet* and locate a file's key to download. *Freenet* provides no search mechanism common to other file sharing systems. A subject desiring to download a file must first find the key on a *Freesite* or message board containing material of interest.

21. This affiant knows from training and experience that streams of requests for blocks of a particular file from an IP address can be evaluated to determine if the IP address is the likely requester of the file.

22. This affiant knows from training and experience that some people who collect child pornography tend to keep the images they obtain for extended periods of time and do not delete the images. They tend to regard the images as trophies and use them for sexual gratification. They also use the collected images and videos of child pornography as bargaining tools when trading child pornography with other individuals. While others delete these images knowing they are able to acquire them again with the use of the internet.

23. This affiant knows from training and experiences that people who tend to collect images of child pornography use video and audio components to capture and record child pornography. They are also known to transfer these images to other digital media storage devices.

24. This affiant knows from training and experience that it is possible to recover digital files forensically even if they have been deleted.

WHEREFORE, your petitioner prays that a search warrant be issued as provided by law.

Det Saughr
(Police Officer) 3562

Sworn and subscribed before me this 18 day of August, 2015, at 1405.

[Signature]
(Judge)

